Intercept and Intelligence Hopefully Lawful

Fred Baker
Cisco Fellow

 © 2001, Cisco Systems, Inc. All rights reserved.

We'll discuss two programs

- **Lawful intercept**
  - Investigation of specific persons
  - Involves disclosure of a person's communications
  - Focuses on the crime/criminal being investigated
- **Forensic intelligence**
  - Investigation of potential events
  - May lead to investigation of persons or groups
  - Focuses on the data being developed

 © 2001, Cisco Systems, Inc. All rights reserved.

Perspective

- No activist view expressed
- Forensic surveillance is a legal requirement of service providers in every country
- I am interested and involved because I have a personal viewpoint:
  - Abide by and support law in a context of privacy

 © 2001, Cisco Systems, Inc. All rights reserved.

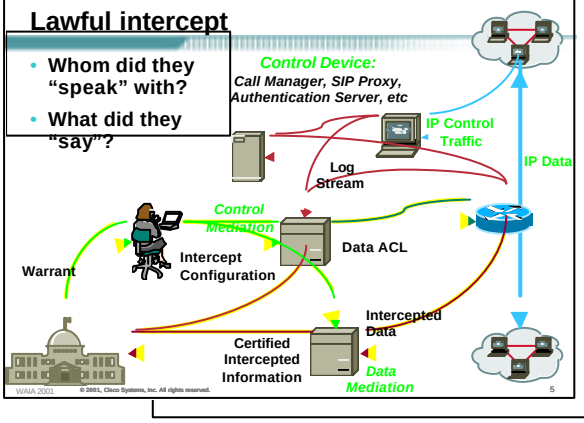
Lawful intercept: surveillance

- Historical capability in telephone network
- Forensic requirements
- Being added to internet
- Issues

 © 2001, Cisco Systems, Inc. All rights reserved.

Lawful intercept

- Whom did they "speak" with?
- What did they "say"?



 © 2001, Cisco Systems, Inc. All rights reserved.

Historical capability in telephone network

- **Pen register**
  - "Whom did he call?"
- **Trap and trace**
  - "Who called him, and where are they?"
- **Content intercept**
  - "What is he saying?"

 © 2001, Cisco Systems, Inc. All rights reserved.

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr

Being added to Internet in most countries

- "Pen register" and "Trap and trace"
  - Real time access to specified event logs
  - May require review of log messages
  - May require reformatting for automated processing
- "Content intercept"
  - Bi-casting traffic into a tunnel
- Concept of "hot pursuit"

 © 2001, Cisco Systems, Inc. All rights reserved.

Log access

- Much of "pen register" tracing is simply access to billing logs
  - In UK, this is not considered a "tap", it is merely forensic procedure
- Such logs generally do not exist in the Internet
  - Billing by month, not by site or URL accessed
  - For example, if question is whether a person is accessing a certain web site or type of site, only web site and personal computer have logs – both of which may be surveillance subjects

 © 2001, Cisco Systems, Inc. All rights reserved.

What is "content"?

- Certainly information that is permanent
- Control information in same message?
- Signaling information? At what layer?

 © 2001, Cisco Systems, Inc. All rights reserved.

"Hot pursuit"

- Telephone systems
  - Traces often report the event of a call
  - Some content necessary to determine who is called (DTMF tones)
- Data systems
  - When is "some" content "delivery of content"?
  - What is the internet corollary of "trap and trace"?

 © 2001, Cisco Systems, Inc. All rights reserved.

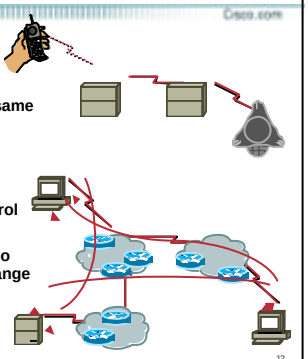
Forensic requirements

- Undetectable by surveillance subject
- "Reliable" or "resilient" delivery transport
- Privacy of data path to LEA
- Certified data
- Often tap of a device
  - Readily defeated by changing devices
  - Denmark and maybe US: tap a person

 © 2001, Cisco Systems, Inc. All rights reserved.

Control and data planes

- Telephone system routing
  - Call control and data follow same path
- Internet access routing
  - Often follows different path
  - Data path may not be in control jurisdiction
  - Many data exchanges have no corresponding control exchange



 © 2001, Cisco Systems, Inc. All rights reserved.

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr

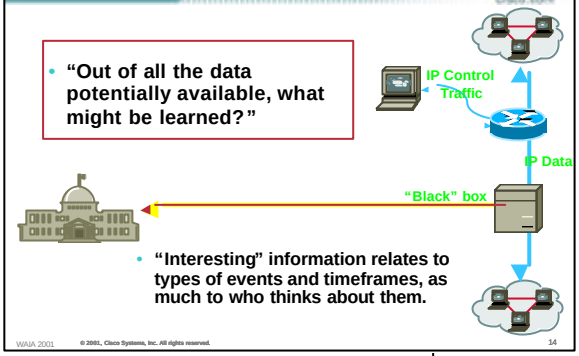
Intelligence: information gathering

- Systems
  - Echelon or Carnivore
- Form of analysis
  - Record data matching some constraint
  - Generally just the record and trace information
- Expected outcome
  - Offline analysis to develop leads

© 2001, Cisco Systems, Inc. All rights reserved.

Intelligence gathering…

- "Out of all the data potentially available, what might be learned?"



- "Interesting" information relates to types of events and timeframes, as much to who thinks about them.

© 2001, Cisco Systems, Inc. All rights reserved.

Where we're headed

- Too early to tell
- Largely a legal question
- Near term
  - Plan on lawful intercept requirements
  - Intelligence requirements in some countries

© 2001, Cisco Systems, Inc. All rights reserved.

Intercept and Intelligence Hopefully Lawful

Fred Baker
Cisco Fellow

© 2001, Cisco Systems, Inc. All rights reserved.

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr